Patent Claims

1. A method for encrypting digital information comprising the following steps:
-using communication devices which have an interface for a replaceable or writable storage medium, whose content may be read out and duplicated,
-using a storage medium which is connected to the interface, a supply of symbols for encryption being stored on the digital storage medium which may be read out on the basis of an address,
-using an encryption unit which employs the supply of symbols for encrypting or decrypting the digital data stream of the communication devices on the basis of at least one address.

2. The method according to the preceding claim, wherein the symbols on the storage medium are only used once and are thus "used up".

3. The method according to one or more of the preceding claims, wherein the symbols are encrypted and decrypted with the data stream using mod2.

4. The method according to one or more of the preceding claims, wherein the mobile terminal is a radio device, laptop, PDA, and/or a mobile telephone which has an interface for a memory card that is insensitive and may be used in portable communication devices.

5. The method according to one or more of the preceding claims, wherein the storage medium is a flash memory

card, a hard drive, or an optical storage drive, whose information may be addressed.

6. The method according to one or more of the preceding claims, wherein the addresses of the symbols to be used on the storage medium are transmitted to synchronize the encryption.

7. The method according to the preceding claim, wherein the addresses are transmitted at specific intervals to synchronize the encryption.

8. The method according to one or more of the preceding claims, wherein there is a first random generator (PRG2) on the communication device which determines the address on the storage medium.

9. The method according to one of the preceding claims, wherein the status of the random generator is transmitted to synchronize the encryption.

10. The method according to one or more of the methods according to the preceding claim, wherein there is a second random generator (PRG1) which performs scrambling of the access to individual segments if PRG2 determines the concrete addresses of the segments.

11. The method according to one or more of the preceding claims, wherein a permutation of the digital data is performed before it is transmitted.

12. The method according to one or more of the preceding claims, wherein the storage medium is written by the noise of an analog source using an A/D converter.

13. A communication device which encrypts a digital data stream,
-having an interface for a replaceable or writable storage medium, whose content may be read out and duplicated, a supply of symbols for encryption, which may be read by using an address, being stored on the storage medium, which may be connected to the interface,
-having an encryption unit, which is set up so that it uses the supply of symbols for encrypting or decrypting the digital data stream of the communication devices by accessing this supply through addresses.

14. The communication device according to the preceding communication device claim, comprising a device which uses the symbols on the storage medium only once.

15. The communication device according to one or more of the preceding communication device claims, comprising a computer which encrypts or decrypts the symbols with the data stream using mod2.

16. The communication device according to one or more of the preceding communication device claims, wherin it is a radio device, laptop, PDA, or a mobile telephone which has an interface for a memory card, the memory card being insensitive and usable in portable communication devices.

17. The communication device according to one or more of the preceding communication device claims, wherein the storage medium is a flash memory card, a hard drive, or an optical storage drive whose information may be addressed.

18. The communication device according to one or more of the preceding communication device claims, comprising means which transmit the addresses of the symbols to be used on the storage medium for synchronizing the encryption.

19. The communication device according to the preceding claim, comprising means which transmit the address at specific intervals to synchronize the encryption.

20. The communication device according to one or more of the preceding communication device claims, wherein there is a first random generator (PRG2) on the communication device which determines the address on the storage medium.

21. The communication device according to the preceding claim, wherein the status of the random generator is transmitted to synchronize the encryption.

22. The communication device according to the preceding claim, comprising means, through which the status of the random generator is transmitted at specific intervals.

23. The communication device according to one or more of the preceding communication device claims, wherein there is a second random generator (PRG1), which

scrambles the access to individual segments if PRG2 determines the concrete addresses of the segments.

24. The communication device according to one more of the preceding communication device claims, comprising means which perform a permutation of the digital data before the data is transmitted.

25. The communication device according to one more of the preceding communication device claims, wherein the storage medium is written by the noise of an analog source using an A/D converter.

26. A use of a mobile addressed memory element, such as a flash card, which is readable by a mobile communication device, for storing symbols for encryption, the symbols being able to be addressed.

27. Software for a communication device, such as a mobile terminal, characterized by the implementation of a method according to one or more of the preceding method claims.

28. A data carrier for a computer, storing a software according to the preceding software claim.

29. A computer system having a communication interface, comprising a device which allows the execution of a method according to one or more of the preceding method claims.